IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

IN RE: DEALER MANAGEMENT SYSTEMS ANTITRUST LITIGATION	MDL No. 2817 Case No. 18 C 864
This Document Relates to: *Authenticom, Inc. v. CDK Global, LLC, et al.*, Case No. 1:18-cv-00868 (N.D. Ill.)	Hon. Robert M. Dow, Jr. Magistrate Judge Jeffrey T. Gilbert **PUBLIC-REDACTED**

AUTHENTICOM'S OPPOSITION TO DEFENDANTS' MOTION TO COMPEL PCM LOG AND CORPORATE TESTIMONY UNDER RULE 30(B)(6)

Plaintiff Authenticom, Inc. respectfully submits this opposition to CDK Global, LLC's ("CDK") and The Reynolds and Reynolds Company's ("Reynolds") motion to compel (1) the production of data from the Polling Client Manager software program, and (2) testimony regarding DataVast, a subject on which Defendants have already obtained hours of testimony and a multitude of documents. As to the first issue, Authenticom has *never* – in the ordinary course of its business or otherwise – maintained or created a report with the information Defendants seek. Requiring Authenticom to do so now – which is not even feasible without hours of engineering and manual work – would contravene the bedrock principle that parties are not required to create documents that have never been created or maintained in the ordinary course of business. Defendants' motion on this issue is also untimely, as the parties hashed these matters out last summer before the August 6, 2018 deadline for filing motions to compel. As to the second issue, Defendants did not properly notice a Rule 30(b)(6) topic on DataVast, and Defendants should not be able to get a second bite at the apple now. Moreover, Defendants have already taken depositions from multiple Authenticom witnesses on DataVast – a product that Authenticom sold off years ago – and

received hundreds if not thousands of documents on the topic. There is no basis to give Defendants yet more discovery now.

At bottom, what this Court stated on January 17, 2019 – when it denied Authenticom's effort to obtain discovery from CDK on two admittedly relevant topics months before discovery ended – applies with even more force now: "In all cases there comes a time when discovery must end. Discovery, like all matters of procedure, has ultimate and necessary boundaries. The discovery rules are not an excursion ticket to an unlimited, never-ending exploration of every conceivable matter that captures an attorney's interest." Dkt. 498 (quotation marks and citations omitted). If those principles applied to Authenticom's efforts to obtain discovery then, they should apply to Defendants' efforts now. The Court should deny Defendants' motion.

I. Authenticom Cannot Be Required to Create Documents With Respect to the Transient Data Within the Polling Client Manager Software Program

For the reasons set forth below, Defendants' motion to compel production of software data that exists within a program called "Polling Client Manager" should be denied.

1. At the outset, it is important to correct Defendants' mischaracterization of the kind of data they seek, and what the Polling Client Manager ("PCM") is. The Polling Client Manager is a software program that Authenticom uses to manage its data extraction processes on behalf of dealers. *See generally* Decl. of Brian Clements. The software program is not a database. Instead, within the application itself, it has a log of activity that is maintained on a day-to-day rolling basis. *Id*. The log is what is considered "transient data," or "ephemeral data," which is data that is created within an application session and then is reset back to its default state after an application session ends. *Id*. This is different from "persistent data," which is data that remains intact from session to session and is typically stored on servers in a database. *Id*. Authenticom has never – in the ordinary course of its business or otherwise – extracted, produced, or otherwise maintained the

"transient data" within the Polling Client Manager software. *Id*. For a person at Authenticom to review the activity within the software, the employee must log in and open up the program itself. *Id*. There is no "report" or "export" of data that Authenticom creates. *Id*. There is no database across which to run a report. *Id*. Nor is it possible for Authenticom to convert the "transient data" within the software program into "persistent data" of the kind that is permanently stored and accessible on servers within a database. *Id*. As explained below, *see infra* pp. 8-9, that would require Authenticom to re-write the Polling Client Manager software and purchase numerous expensive servers, which is cost-prohibitive. *Id*. In short, Authenticom has *never* – in the ordinary course of its business or otherwise – created a report of the seven-day rolling transient data within the Polling Client Manager. *Id*. And without re-programming the software program, such reports *cannot be run*. The information sought can only be viewed within the software program itself. *Id*.

2. It is black letter law that parties are under no obligation to create physical or electronic information that is not maintained in the ordinary course of business. Federal Rule 34 only "contemplates production of documents already in existence and does not require a party to create or prepare" documents or information. *See Sullivan v. Conway*, 1995 WL 573421, at *4 (N.D. Ill. Sept. 27, 1995); *United States v. Rebolledo-Delgadillo*, 2015 WL 13037308, at *6 (N.D. Ill. April 14, 2015) ("No party has an obligation to create evidence"). Federal courts are unified on this point. *See, e.g.*, *Turner v. Rataczak*, 2014 WL 834721, at *3 (W.D. Wis. Mar. 4, 2014) ("[C]ourts may not compel a party to create new documents solely for their production in response to a Rule 34 request.") (citation and quotation marks omitted) (citing cases); *Int'l Bus. Machs. Corp. v. BGC Partners, Inc.*, 2013 WL 1775437, at *1 (S .D.N.Y. Apr. 25, 2013) ("Parties are only required to produce documents that exist; they have no obligation to create documents to support their adversary's theory of the case."); *A.R. Arena Prods., Inc. v. Grayling Indus., Inc.*,

2012 WL 2953214, at *10 (N.D. Ohio Apr. 30, 2012) ("Courts have consistently held that a party cannot be compelled to create, or cause to be prepared, new documents solely for their production. Rule 34 only requires a party to produce documents that are already in existence.") (internal quotations marks omitted); *Alexx, Inc. v. Charm Zone, Inc.*, 2010 WL 11574190, at *2 (N.D. Cal. Apr. 30, 2010) (a party is under "no obligation to create electronic documents"; "it is only obligated to produce the documents as they are kept in the normal course of business").

Furthermore, as noted above, the transient data within the Polling Client Manager is not in a database or format that can be exported and produced: the data exists within the software itself and resets to a default state on a seven-day rolling basis. *See supra* pp. 2-3. Thus, this is not a situation where a query can be run across a database. Rather, Authenticom would have to compile and create the dataset itself, which it has no duty to do. *See Ahad v. Bd. of Trustees of S. Ill. Univ.*, 2018 WL 534158, at *5 (C.D. Ill. Jan. 24, 2018) ("Pulling information from a database and organizing it into a readable spreadsheet is a far different task than compiling and creating the dataset itself" and Rule 34 only requires a party to "produce documents as they are kept in the usual course of business or organize and label them to correspond to the categories in the request.").

To use an apt analogy offered by one court, Defendants' request is akin to telling Authenticom that it must reconfigure its telephones to record employees' conversations. Nothing in the Federal Rules creates any such obligation. *See Louis Vuitton Malletier v. Dooney & Bourke, Inc.*, 2006 WL 3851151, at *2 (S.D.N.Y. Dec. 22, 2006) (no duty to save chatroom conversations; describing movants' arguments as "akin to a demand that a party to a litigation install a system to monitor and record phone calls").

In addition, even putting aside the fact that Defendants' requests impermissibly require Authenticom to create new documents, those requests are disproportionate to the needs of the case given the burdens involved. *See* Fed. R. Civ. P. 26(b)(1). The ephemeral PCM data at issue here is "not reasonably accessible because of undue burden or cost." Fed. R. Civ. P. 26(b)(2)(B). Accordingly, Defendants are entitled to discovery only if they can "show[] good cause, considering the limitations of Rule 26(b)(2)(C)." Fed. R. Civ. P. 26(b)(2)(B). No such good cause exists here. As the Seventh Circuit's Electronic Discovery Committee stated, ephemeral data "generally are not discoverable in most cases." *See* Seventh Circuit Electronic Discovery Committee, Principles Relating to the Discovery of Electronically Stored Information, Principle 2.04(d) (Aug. 1, 2010), available at: https://www.ediscoverycouncil.com/sites/default/files/Principles8_10.pdf.

Likewise, the Sedona Conference Working Group has stated: "Absent a showing of special need and relevance, a responding party should not be required to preserve, review, or produce deleted, shadowed, fragmented, or residual electronically stored information." *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 Sedona Conf. J. 1, 144 (2018) (Comment 9).

These general principles have even more force here given the undue burdens on Authenticom. As the notes to the 2015 amendments to Rule 37 state: "Another factor in evaluating the reasonableness of preservation efforts is proportionality. The court should be sensitive to party resources; aggressive preservation efforts can be extremely costly, and parties (including governmental parties) may have limited staff and resources to devote to those efforts." Advisory Committee note to 2015 Amendments to Fed. R. Civ. P. 37(e). As explained above, and more fully in the accompanying declaration of Brian Clements, *see* Ex. 1, employees at Authenticom would have had to spend numerous engineering hours to figure out how to obtain the transient data

from the program and then many more hours manually constructing it into a useable format for production. Authenticom is a small business – not a multi-billion dollar behemoth like Defendants – and its business has already been decimated by Defendants' anticompetitive conduct. It would be wildly disproportionate to say that Authenticom should have spent extensive employee time and expense reconfiguring its PCM system to create records of the ephemeral data that Defendants now want.[1]

3. Defendants' motion can also be denied on the ground that it is untimely. In multiple meet and confers and letters from May through August 2018, Authenticom explained these matters to Defendants: that the Polling Client Manager only maintains seven-days' worth of transient data; that Authenticom would not produce the information; and "that it has not and cannot preserve the transient data." *See* Ex. 2 (May 23, 2018 letter from Leo Caseria to M. Nemelka); Ex. 3 (May 25, 2018 letter from M. Nemelka to B. Miller, B. Ross, and L. Caseria); Ex. 4 (June 5, 2018 letter from L. Caseria to M. Nemelka and P. Wedgworth); Ex. 5 (July 27, 2018 letter from M. Nemelka to L. Caseria); Ex. 6 (Aug. 2, 2018 letter from M. Nemelka to L. Caseria). Therefore, if Defendants wanted to move to compel on this issue, then under the Case Management Order, Defendants were required to do so by August 6, 2018. *See* Dkt. 166 (setting August 6, 2018 as the "Deadline to file Motions to Compel, if any, after strict compliance with Local Rule 37.2"). Defendants have no

[1] Authenticom timely objected to Defendants' document requests on this ground, including the specific requests at issue. *See*, *e.g.*, Ex. 7, Authenticom's Objections and Responses to Defendant CDK Global, LLC's First Requests for the Production of Documents at 7 (Response to RFP No. 2: "Authenticom further objects to this Request on the grounds that it seeks the production of documents that may not be maintained in the fashion requested and would require Authenticom to create documents not presently in existence."); *id*. at 4, General Objection and Response No. 19 ("Authenticom disclaims any suggested obligation to create documents in response to the Requests."). Defendants made similar objections to Plaintiffs' document requests and refused to create documents that they did not otherwise create or maintain in the ordinary course of business. Defendants are thus asking Authenticom to do something they themselves have disclaimed any duty to do.

excuse for failing to file a timely motion to compel where this issue was raised and fully hashed out prior to the motion deadline. Compounding the problem, Defendants waited until after the close of discovery to file the instant motion to compel, which makes the motion doubly untimely. *See In re Sulfuric Acid Antitrust Litig.*, 231 F.R.D. 331, 332 (N.D. Ill. 2005) ("In one regard, however, a line of sorts has been sketched by a series of decisions: motions to compel filed after the close of discovery are almost always deemed untimely."). Therefore, not only is Defendants' motion wrong on the merits, it is also untimely for multiple reasons.[2] Defendants' motion should be denied.

4. Defendants' motion is also a breach of a discovery agreement that the parties reached in the summer of 2018. Indeed, this is a classic example of no good deed going unpunished. After Authenticom explained in the summer of 2018 to Defendants that it would not and could not provide the transient data from the Polling Client Manager, *see supra* p. 6, the parties reached a compromise: instead of providing the data from the Polling Client Manager, the parties agreed that Authenticom would provide a log of when dealer data was "ingested" into Authenticom's system. *Id*. Authenticom made the offer "in a spirit of compromise and in a good faith effort to reach resolution on these issues." Dkt. 710-14 (Defs.' Ex. 14). Defendants confirmed the agreement on August 3, 2018, before the motion to compel deadline: "With respect to the DMS access log that we've been discussing, which you offered to create and produce, please

[2] It is worth noting that Plaintiffs made sure not to make the same mistake. On August 6, 2018, Plaintiffs filed a motion to compel Defendants to produce documents related to their provision of data integration services to OEMs. *See* Dkt. 316. The Court denied Plaintiffs' motion, but invited them to file a renewed motion if discovery provided more evidence for the relevance of the OEM data. *See* Dkt. 441. Discovery did provide such information; Plaintiffs met and conferred with Defendants; and receiving an inadequate response from Defendants, Plaintiffs filed the renewed motion to compel before the close of discovery. *See* Dkt. 663. With deadlines, one set of parties should not be required to play by the rules while the other side gets a free pass.

do so." Dkt. 710-15 (Defs.' Ex. 15). Relying on that agreement, Authenticom spent a huge amount of effort and created the "ingestion" log, and provided it to Defendants before the document production deadline of October 12, 2018. To Authenticom's dismay, after Defendants induced Authenticom to undertake the effort to create and provide the "ingestion" log, Defendants then asked for Authenticom to provide the data from the Polling Client Manager. On November 16, 2018, Authenticom responded that "after the parties reached agreement on this issue, after Authenticom undertook extensive work to create the [ingestion] log, and after Authenticom produced the log," it was a breach of the discovery agreement to "now insist on any further discovery with respect to the PCM Logs." Ex. 8 (Nov. 16, 2018 letter from M. Nemelka to R. MacDonald); *see also* Dkt. 710-19 (Defs.' Ex. 19). Nevertheless, on December 7, 2018, "in a further effort to address Defendants' demands, we have been investigating whether it is possible to create an example of a PCM Log." *Id*. In a show of good faith, Authenticom manually created that example for a dealership, and provided it to Defendants. *See* Defs.' Mot. at 5-6. Now Defendants want more – they want a full rolling seven-day example of the transient data that Authenticom has told them since May 2018 that it could not and would not provide. And yet, in a further show of good faith, Authenticom has offered to manually create Polling Client Manager records for twenty randomly selected dealers. While that would be a laborious effort, Authenticom was willing to do it to resolve the issue, but Defendants rejected that olive branch. In short, Defendants' breach of their discovery agreement is an independent basis to deny Defendants' motion.

5. Finally, Defendants' suggestion (at 1-4) that Authenticom has "purged" the transient data within the Polling Client Manager software is a gross misstatement and cannot go unrebutted. As Authenticom fully explained to Defendants in letters and during meet and confers,

see supra p. 6, converting the "transient data" within a software program into "persistent data" of the kind that is permanently stored within a database on physical servers is impossible for Authenticom. At a minimum, Authenticom would have to rewrite the Polling Client Manager software. *See* Ex. 1 (Decl. of Brian Clements), ¶ 7. That would require the efforts of Authenticom's entire technical development staff – already depleted to a handful of employees after the layoffs – to what could be a futile effort. *Id*. And even if the software could be rewritten to convert the transient data to persistent data, Authenticom would have to purchase a huge number of new servers to store that data. *Id*. Authenticom has no financial resources to do that. *Id*. Defendants' accusation (at 4) that Authenticom is "purging" data is unfair and inaccurate.[3]

Moreover, without fully engaging with Defendants' footnote suggestion that Authenticom's conduct constitutes spoliation, Authenticom notes that, prior to the 2015 amendments, Rule 37 specifically created a safe-harbor for ESI that is "lost as a result of the routine, good-faith operation of an electronic information system." Fed. R. Civ. P. 37. The 2015 amendments substituted a flexible standard for a rigid safe-harbor, but they were not intended to override the basic principle that loss of ESI that is over-written or not retained in the course of the good-faith operation of a computer system is not spoliation. Indeed, as discussed above, the 2015 amendments specifically highlighted the burdens of the types of "aggressive" preservation measures that Defendants apparently assert that Authenticom should have engaged in here.

[3] Defendants also allude (at 2-3) to certain "methods Authenticom used to wrongfully access Defendants' DMSs" that have no bearing on their motion, and were included in an ostensible effort to malign Authenticom. Suffice it to say that – like the accusation that Authenticom has "purged" the transient data – Defendants' descriptions are inaccurate and leave out material information. These are matters for summary judgment, not this discovery motion.

II. Defendants' Rule 30(b)(6) Notice to Authenticom Did Not Include a Topic on DataVast, and Defendants Have Already Taken Extensive Discovery on the Subject

Rule 30(b)(6) allows a party to depose an organization if it "describe[s] with reasonable particularity the matters for examination." Fed. R. Civ.P. 30(b)(6). But Defendants failed to do that with respect to DataVast, and they are now attempting to get a second bite at the apple through this motion. Moreover, Defendants have already received extensive discovery on DataVast – over the course of multiple depositions and through document discovery – and there is no basis for more. Finally, counsel's instructions during the 30(b)(6) deposition to freely answer any question, but with the guidance not to reveal attorney-client work product and communications in the process, were standard and proper.

1. [redacted]

DataVast is not mentioned once in the entirety of Defendants' Rule 30(b)(6) notice to Authenticom – not in any instruction; not in any definition; and most certainly not in any topic. Defendants (at 8) make a half-hearted effort to shoehorn their questions on DataVast within the topic on Authenticom's efforts "to secure or protect 'dealer data'," but it does not fit. Defendants asked hours of questions about Authenticom's security practices, security protocols, and steps

Authenticom takes to protect dealer data, and the witness answered those questions at length. Questions about a former marketing company for dealers does not fall within that fair scope of that topic. Neither does it fall within the other topic Defendants cite, namely, Topic 7 which covers "agreements with third-party vendors to obtain data maintained on a CDK or Reynolds DMS." Defs.' Mot. at 8. It is not even clear what this topic has to do with DataVast, and Defendants do not elaborate in their motion. Indeed, when Defendants identified in writing which topics they thought covered DataVast, they did not even cite this topic. Ex. 9 (April 18, 2019 email from M. Stein to M. Nemelka). Similarly, when Authenticom asked Defendants on the record at the deposition which topic covered DataVast, counsel for Defendants did not cite this topic on "agreements with third-party vendors" either. Tellingly, Defendants' motion is the first time they have cited Topic 7 as covering DataVast. In short, Authenticom had no notice that Defendants would ask about DataVast at the 30(b)(6) deposition. If Defendants believed that they needed to ask questions about it, then they could have written a topic on it, but they did not, and the Court should not give them a do-over.

Defendants' efforts to get a second bite at the apple are also unnecessary because they have already taken multiple Authenticom depositions on the subject. For example, the depositions of Russell Gentry (Authenticom's former President) and Travis Robinson (Authenticom's former CFO) were largely spent on the topic of DataVast and related subjects. Defendants have also received hundreds if not thousands of documents on DataVast. In such situations, courts routinely deny a party's efforts to get yet additional discovery through a Rule 30(b)(6) deposition. *See Smithkline Beecham Corp. v. Apotex Corp.*, 2000 WL 116082, at *10 (N.D. Ill. Jan. 24, 2000) (denying motion to compel responses to 30(b)(6) topics where requesting party "failed to convince [the court] that the factual information they seek has not already been produced, or that it cannot

be discovered through a less invasive method"); *id*. ("[T]he recipient of a Rule 30(b)(6) request is not required to have its counsel muster all of its factual evidence to prepare a witness to be able to testify regarding a defense or claim. This rule holds especially true when the information sought is likely discoverable from other sources.") (internal citations omitted). Defendants' motion to compel should therefore be denied.

2. Authenticom designated Dane Brown, its general counsel, as the 30(b)(6) witness. Mr. Brown thoroughly prepared for his deposition over the course of many days, and Defendants have raised no issue with his preparation or testimony on the actually noticed topics. But because DataVast was not a noticed topic, Mr. Brown explained on the record that his preparation to serve as Authenticom's corporate witness did not include the subject. Dkt. 711-9 (Defs. Ex. 9) (D. Brown Dep. Tr. at 224:11-20). Accordingly, counsel for Authenticom provided the following guidance to Mr. Brown with respect to the few questions on DataVast that Defendants asked: "You can answer that, if you know . . . and if you can answer that without revealing attorney-client communications" or "your attorney-client work for Authenticom." *Id.* (D. Brown Dep. Tr. at 223:1-6, 225:11-20). Mr. Brown – who joined Authenticom in May 2016 well after Authenticom had sold DataVast – stated that he could not answer the questions without breaking the privilege. *Id*. (D. Brown Dep. Tr. at 224:5-9. The basis of the privilege, as the witness established on the record, was both his "work as Authenticom's general counsel," and "based on communications with outside counsel." *Id*.

Based on the foregoing, the instructions to the witness by Authenticom's counsel were standard and proper. It is well-established "that a question calling for privileged matter need not be answered. To answer subject to an objection of privilege could destroy the privilege." *Eggleston v. Chicago Journeymen Plumbers' Local Union No. 130, U. A.*, 657 F.2d 890, 902–03

(7th Cir. 1981); *Papst Licensing GmbH & Co. KG v. Apple, Inc.*, 2017 WL 1233047, at *7 (N.D. Ill. Apr. 4, 2017) ("If the questions to be asked of [corporate counsel] delve into privileged areas then his recourse will be to object and refuse to answer.") (internal citation omitted). Accordingly, the instruction to the witness that he "can answer that, if you know," while cautioning not to break the privilege, was standard and proper.

Dated: June 8, 2019

Respectfully submitted,

/s/ Derek T. Ho

Derek T. Ho
KELLOGG, HANSEN, TODD, FIGEL & FREDERICK, P.L.L.C.
1615 M Street, NW, Suite 400
Washington, D.C. 20036
(202) 326-7900
dho@kellogghansen.com

Co-Lead MDL Counsel and Counsel for Authenticom, Inc.

CERTIFICATE OF SERVICE

I, Derek T. Ho, an attorney, hereby certify that on June 8, 2019 I caused a true and correct copy of the foregoing **AUTHENTICOM OPPOSITION TO DEFENDANTS' MOTION TO COMPEL PCM LOG AND CORPORATE TESTIMONY UNDER RULE 30(B)(6)** to be filed and served electronically via the court's CM/ECF system. Notice of this filing will be sent by e-mail to all parties by operation of the court's electronic filing system or by email to anyone unable to accept electronic filing as indicated on the Notice of Electronic Filing. Parties may access this filing through the court's CM/ECF system.

/s/ Derek T. Ho

Derek T. Ho
KELLOGG, HANSEN, TODD, FIGEL &FREDERICK, P.L.L.C.
1615 M Street, NW, Suite 400
Washington, D.C. 20036
(202) 326-7900
dho@kellogghansen.com